UNIT 1 NETWORKING AND INTERNET

Structure

1.0 INTRODUCTION

As discussed in the previous blocks, the initial computers were designed as a machine that could perform monotonous arithmetic calculations with ease and lot of accuracy. The computing power of the computers kept on increasing every year while during the same time the technologies of message transfer were advancing. During the era of 1960-70, the computers were becoming faster, cheaper but more powerful and smaller in size. The number of application of the Computer also kept growing, however, the main breakthrough that enhanced the use of Computer was the advent of network of interconnected computers. The Computer Network made various computers to share information at a very high speed.

The Internet

In the year 1960, the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defence and researchers from Universities and research centres developed a network called the ARPANET. The main goal of ARPANET was to share data and processing time over a set of computers connected through telephone lines and satellite links. This led to creation of one of most widely used network of networks – the Internet. The Internet could carry any digital signals such as text, graphics, sound, video and animation. Today, Internet has thousands of networks and millions of users, with the numbers expanding daily.

This unit introduces you to some of the basic fundamentals of Computer Networks and the Internet.

1.1 OBJECTIVES

After going through this unit, you should be able to:

- define the basic concepts of networking;
- discuss the basic models of networks;
- explain different types of networks;
- differentiate among different networking devices;
- explain the addresses used on the Internet; and
- explain the different advantages of networks.

1.2 WHAT IS A COMPUTER NETWORK?

A computer network can be simply defined as the interconnection of two or more independent computers. Applications of computer networks are found everywhere. They are used in our homes, schools, colleges, railway stations, offices and business. They help us to send an email, watch a live sports event at our computer, book rail/air tickets and do chatting with our friends. **But why do we need Networks?**

1.2.1 Advantages of using Computer Networks

We use a Computer Network for the following reasons:

a) **Resource sharing**: A network is needed because of the desire to share the sharable programs, data, and equipment available to anyone on the network without regard to the physical location of the resource and the user. You can also share processing load on various networked resources.

b) **High reliability**: A network may have alternative sources of supply (e.g., replicated files, multiple CPUs, etc.). In case of one resource failure, the others could be used and the system continues to operate at reduced performance. This is a very important property for military, banking, air traffic control, and many other applications.

c) **Cost-benefit advantage**: A network may consist of many powerful small computers, one per user. You can keep the data and applications on one or more shared and powerful file server machines. This is called the client-server model. Such model offers a much better price/performance ratio than old mainframes. At present many server services have been moved to Internet based resources set up by a third party and shared by many (called cloud). This allows users to use powerful server applications and data services without maintaining servers. Such system may bring down the cost further. However, such models still have several issues that are being debated.

d) **Scalability**: The ability to increase system performance gradually by adding more processors (incremental upgrade).

e) **Powerful communication medium**: Networks make cooperation among far-flung groups of people easy where it previously had been impossible.

In the long run, the use of networks to enhance human-to-human communication may prove more important than technical goals such as improved reliability.

One of the most popular application of network is the World Wide Web which is an application of Internet. Let us introduce you to internet in the next subsection.

1.2.2 The Internet

Internet is an interconnection of thousands of networks. It came into being in 1967. Internet has a very interesting history. You can trace the evolution of Internet at the website *http://www.wikipedia.com* . One of the major applications of the Internet is the World Wide Web (WWW). Internet and WWW (World Wide Web) are often used as synonyms of each other, which is technically not correct as the Web is a collection of interconnected documents and other resources. WWW was started in 1989 by Sir Tim Berners-Lee at Physics Laboratory (CERN).The WWW provides a “point-and-click” interface to text, images, sound and movies that has proven to be very easy-to-use. This feature was made available due to Hypertext that provides a “point and click” link to other documents on the WWW. To access the information on internet you require a software called web browser. Some of the popular browser software are - Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari etc.

The Internet is a collection of various services, tools, applications and resources. Some of the popular services on the internet are – browsing, searching, e-mail, chat, e-learning and lots more. Today, Internet has brought the world on your desktop. Right from news across the world, wealth of knowledge to shopping, purchasing the movie, railway or air tickets everything is at your mouse click. It has also become the most excellent business tool of modern scenario. Several activities can be performed if you have access to the Internet; like you can use it for learning or teaching, you can be part of an online distributed project, you can use it for publicity and advertisement, you can refer Internet for career or job consultation and so on. Unit 2 and Unit 3 discuss some of the services tools, applications and resources available on the Internet in more details.

Before we discuss more about Internet, first let us describe the process of data communication system that forms the core of computer network.

1.2.3 Data Communication System

In the connected world, a computer does not work as a standalone system but as part of a communication system. Besides computers, most of the large/complex systems like the navigation systems for ships or aircraft or rockets, the satellites and many other systems rely on the communication system. In the most fundamental sense, communication involves implicitly the transmission of data or information (the information is derived from data) from one point to another through a succession of processes. Data is transmitted over any communications medium as either *digital* or *analog* form. The most important factors affecting the transfer of a signal over a medium are noise and attenuation. Noise is the external disturbances whereas attenuation is defined as degeneration of the signal. A simple communication system can be represented by the block diagram shown in Figure 1.1.

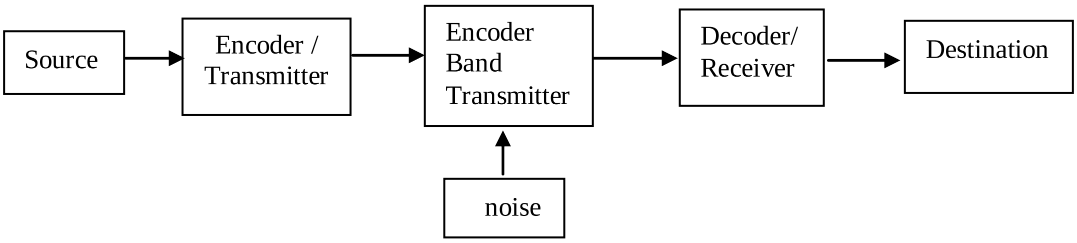


Figure 1.1 : A Simple Communication System
(Source: PhD thesis of Professor Manohar Lal)

The communication system essentially consists of five parts:

Source: Source produces a message or sequence of messages to be communicated to the receiver. The source output may be in many different forms such as a waveform, a sequence of binary digits, and a set of output from sensors in a space probe, or many other similar forms.

An Encoder: Encoder represents any processing of the source messages/ signals prior to transmission. The processing might include, for example, any combination of modulation (discussed in later section), data reduction and insertion of redundancy to combat the channel noise.

The Channel: Channel is the medium for transmitting signals from transmitter to receiver. It may be a telephone line, a high frequency radio link, a space communication link or a storage medium. A channel is usually subject to various types of noise disturbances, which on telephone line, for example, might take the form of a time-varying frequency response, crosstalk from other lines, thermal noise, and impulsive switching noise. A channel subject to noise is called noisy channel. An error-correcting code corrects errors due to noise.

The Decoder: A decoder represents the processing of a channel output received from the channel to produce an accepted replica of the input at the destination.

The Destination: Destination is the receiver. It may be the person or object for whom the message is intended.

An example of communication system: Suppose a student computer is connected through a modem to a telephone line. If she/he wants to send a file to his/her friend over a communication system, his/her computer is the source, the modem converts his digital file into analog signal that can be transmitted over the telephone line to the receiver’s modem which at its end converts the signal back to the digital signal. The digital data then is accepted by the destination computer.

Some standard data transmission concepts are:

- The data in a communication system may be transmitted as analog or digital data over a single path serially or number of parallel paths.
- The data can be sent asynchronously when both the source and receiver are not following timing or synchronously when both sender and receiver agree on the sequence of arrival of data.
- *Modes of Data Transmission:* There are 3 modes of data communication:
  - Simplex
  - Half duplex
  - Full duplex

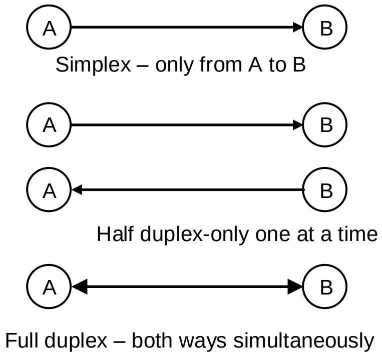

A
B
Simplex – only from A to B
A
B
A
B
Half duplex-only one at a time
A
B
Full duplex – both ways simultaneously

Figure 1.2 : Modes of transmission

Simplex Mode : In simplex mode of data communication, data flow is uni-directional. This means that data travels only in one direction i.e., from a sender to a receiver. The receiver cannot respond back to the sender. An example of simplex mode is keyboard, or a television station telecasting a program.

Half Duplex Mode: Half duplex communications occurs when data flows in both directions; although in only one direction at a time. An example of a half-duplex system is a Walkie-Talkie system used a two-way radio normally by Police. You may use the word "Over" to indicate the end of transmission, and ensure that only one party transmits at a time. In such systems sender and receiver both transmit on the same frequency.

Full Duplex Mode: In full duplex mode of data transmission, data is transmitted in both the direction simultaneously. This means that both the devices in a network can send and receive the data at the same time. It is like a two lane road with traffic moving in both directions at the same time. In this mode signals going in either direction share the capacity. Half of the bandwidth is used for sending data in one direction, while the other half is used for receiving data from other direction. An example is a telephone conversation.

- **Speed of transmission**: Speed of data transmission plays a major role in data communication. How fast data can be transmitted from place to place is sometimes called bandwidth. **Bandwidth** is a data transmission rate that tells the maximum amount of information (bits/second) that can be transmitted along a channel. It is measured in kilobits, kbps, 1,000 of bits per second, or megabits (Mbps), millions of bits per second. Actual transfers are considerably lower because of software and protocol overheads.
- **Some Sample Transmission Speed:** Dial-up modems are generally capable of a maximum bit rate of 56 kb/s (kilobits per second) and require the full use of a telephone line—whereas broadband technologies support at least double this bandwidth. Broadband usually has a high rate of data transmission. In general, any connection to the customer of 256 kb/s (0.256 Mb/s) or greater is more concisely considered broadband Internet.
- **Packet, and Circuit Switching:** This terminology has started from telephone network, where switching offices were places having switches that were used to create connection from one source to destination. Circuit switching involves creating a switched path for entire communication, for example, when you make a telephone call the connection is established by switching and is available for the whole communication. Whereas in packet switching a message is broken in small packet which are handed over from a source to destination through many small steps.

A Computer Network although works on the basic communication system, but is much more than that. It is characterized by a number of tasks that are mostly implemented with the help of networking software that takes care of addressing, routing and reliable delivery of messages. These software are implemented as a number of protocols which are discussed later in the Unit.

What should you know about a computer network?

A computer network requires that the computers must somehow be connected with each other. Thus, you require a physical connection between two or more computers. This connection may be through physical wired media or wireless medium. In addition, it will require certain devices that will enable the connection. These concepts are explained in brief in section 1.3 and 1.7

A related question here is: Are the computer in networks connected arbitrarily or there exists some architecture and structure? Section 1.4 and 1.5 provide details of some simple topological structures and network architectures for networks. It also details the classification of networks.

Another related point is how the data will be transmitted over these connections. We have provided some information on these points in section 1.2.3. For more details on these topics you should refer to the further readings.

Finally, one of the major issues is how two computers will be able to exchange information over the network. This will require discussion on the term protocols and networking software. Section 1.6 and 1.8 covers some basic concepts of these. For more details, you may refer to further readings.

1.3 DATA TRANSMISSION CHANNELS

The data transmission has to be done over a transmission channel or media. It can be classified as:

a) Guided Channels

b) Unguided Channels

1.3.1 Guided Media

Guided media provide a physical connection between two devices. A signal traveling through guided media is directed and contained within the physical limits of the medium. There are several different Guided media, however we define only the most popular as given below:

a) Twisted pair cable

b) Optic Fiber cable

a) Twisted Pair Cable

Twisted pair cable is still the most common transmission media. A twisted pair cable consists of two conductors which are normally made of copper. Each conductor has its own plastic insulation typically 1 mm thick. These cables are twisted together. The wires are twisted in a helical form, similar to a DNA molecule. Twisting is done to reduce crosstalk. Twisted Pairs (Figure 1.3) are very effective for relatively short distances (a few hundred feet), but can be used for up to a few kilometers. A twisted pair has a bandwidth to distance ratio of about 1 MHz per kilometer. The performance of the twisted pair can be substantially improved by adding a metallic shield around the wires. Shielded wires are much more resistant to thermal noise and crosstalk effects. Twisted pairs are used for long distance connections e.g. telephone lines which are usually organized as larger cable containing numerous twisted pairs.

Twisted pair cabling comes in several varieties, two of which are very important: Category 3 and Category 5. Category 5 has more twists per centimeter resulting in less crosstalk and a better quality signal.

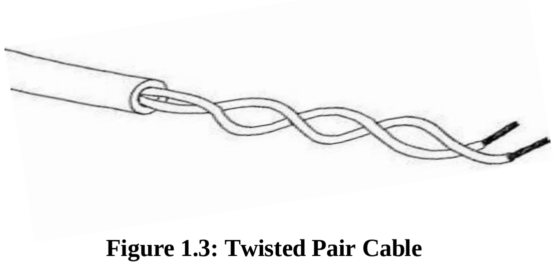


Figure 1.3: Twisted Pair Cable

b) Optical Fiber

An optical fiber consists of two concentric cylinders: an inner core surrounded by a cladding. Both the core and the cladding are made of transparent plastic or glass material as shown in the Figure 1.4, which transmit signals in the form of light. Optical fiber use reflections to guide light through a channel. The density of the core and cladding must differ sufficiently to reflect the beam of light instead of refracting.

The core is used for guiding a light beam, whereas the cladding (which has a different refractive index) acts as a reflector to prevent the light signal instead of electrons, it does not suffer from the various noise problems associated with electromagnetic signals. The signal is usually generated by a laser or Light Emitting Diode (LED). Optical fibers can provide bandwidth to distance ratios in order of 100s of MHz per kilometer. Like other cables, hundreds of optical fibers are usually housed within one cable.

They are being increasingly used as telecommunication carriers for long distance digital trunk lines. Current trends promise that they will replace twisted pair residential loops in the near future.

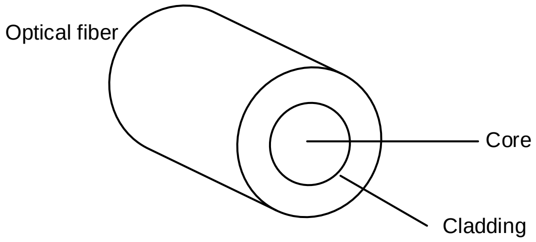


Figure 1.4 : Optical Fiber Cable

Advantages

1) Higher Band width – it can support higher band width and hence can transfer data at a higher rate.
2) Less signal attenuation – its transmission distance is greater than the twisted pair and it can run for 50Kms without regeneration.
3) Immunity to electromagnetic interface
4) These cables are much lighter than the copper cables
5) These cables are more immune to tapping than the copper cables.

Disadvantages

1) Installation or maintenance – it needs expertise which is not available everywhere.
2) Unidirectional – Propagation of light is unidirectional and we need two fibers for bidirectional communication.
3) Costly – the cables and interfaces used are relatively expensive.

1.3.2 Unguided Media

Unguided media is used for transmitting the signal without any physical media. It transports electromagnetic waves and is often called wireless communication. Signals are broadcast through air and received by all who have devices to receive them. It can be categorized as follows:

a) Radio waves
b) Micro waves
c) Infrared

a) Radio Waves

Electromagnetic waves ranging in frequencies between 3 Kilo-Hertz and 1 Giga-Hertz are normally called radio waves. Radio waves are easy to generate and can travel long distances and can penetrate buildings easily, therefore widely used for communication. These are omni-directional which implies that these travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically.

Radio signals have been used for a long time to transmit analog information. They are particularly attractive for long distance communication over difficult terrain or across the oceans, where the cost of installing cables can be too prohibitive.

An increasingly-popular form of radio is cellular radio, which is currently being used by carriers for providing mobile telephone networks. These operate in the VHF (Very High Frequency) band and subdivide their coverage area into conceptual cells, where each cell represents a limited area which is served by a low-power transmitter and receiver station. As the mobile user moves from one cell area to another, its communication is handed over from one station to another. Radio waves transmitted by one antenna are susceptible to interference by another antenna due to its Omni-directional property. Radio waves can be received both inside and outside the building.

Radio waves are very useful in multicasting and hence used in AM and FM radios, cordless phones and paging. You may be wondering about the term multicasting. If the communication is between single source and destination then it is called unicast; on the other hand, if one source is transmitting signal and any destination that is in the range may be able to reach it then it is called broadcast. Multicast is when a source transmits a signal for some specific group of destinations which may be more than one.

Bluetooth: Bluetooth is a very popular application of short wave length radio transmission in the frequency band of 2400 to 2480 MHz. It is a proprietary wireless technology standard used for exchanging data over short distances in mobile phones and other related devices. It allows wireless devices to be connected to wireless host which may be a computer over short distances. You may have it for transferring data between a mobile phone and a computer provided both have Bluetooth technology.

b) Microwaves

Electromagnetic waves ranging from 1 to 300 Gigahertz are called microwaves. Microwaves are unidirectional that is the sending and receiving antennas need to be aligned.

Microwave is by far the most widely used form of radio transmission. It operates in the GHz range with data rates in order of hundreds of Mbps per channel. Telecommunication carriers and TV stations are the primary users of microwave transmission.

An important form of microwave system is a satellite system, which is essentially a microwave system plus a large repeater in the sky as shown in Figure 1.5. The signals transmitted by earth stations are received, amplified, and retransmitted to other earth stations by the satellite. Like other microwave systems, the bandwidth is subdivided into channels of 10s of MHz each, providing data rates in order of 100s of mbps. Because of their high bandwidths, satellites are capable of supporting an enormous number and variety of channels, including TV, telephone, and data. The satellite itself, however, is a major investment and typically has a limited lifetime (at most a few decades).

Unidirectional property of microwave helps in avoiding interference by a pair of aligned antenna to another. High frequency micro waves cannot be received inside the building.

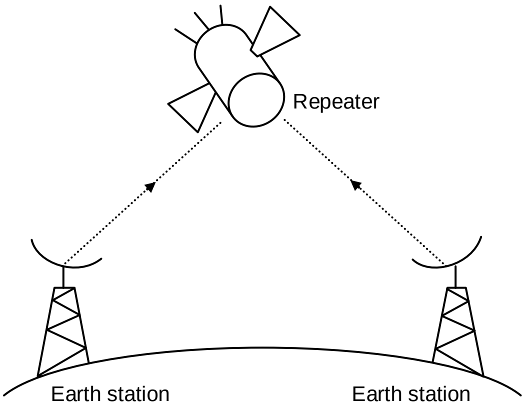


Figure 1.5: Microwaves

c) Infrared

Infrared signals range between 300 Giga-Hertz to 400 Tera-Hertz. These can be used for short range communication. High range infrared rays cannot be used for long range communication as it cannot penetrate walls. This also helps in avoiding interference.

Infrared signals are generated and received using optical transceivers. Infrared systems represent a cheap alternative to most other methods, because there is no cabling involved and the necessary equipment is relatively cheap. Data rates similar to those of twisted pairs are easily possible. However, applications are limited because of distance limitations (of about one kilometer). One recent use of infra-red has been for interfacing hand-held and portable computing devices to Local Area Networks as shown in Figure 1.6.

It cannot be used outside building as rays of sun contain infrared which leads to interference in communication. Infrared having wide bandwidth can be used to transmit digital data with a very high data rate. Infrared signals can be used for communication between keyboards, mouse and printers.

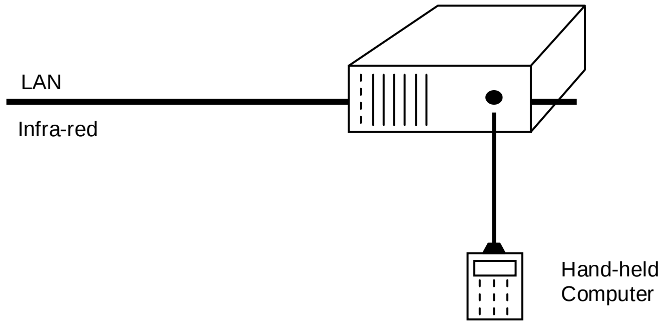


Figure 1.6: Infra Red

Check Your Progress 1

1. What is the need of computer networks?

   …………………………………………………………………………………

   …………………………………………………………………………………

2. In the context of communication system, what does a MODEM do?

   …………………………………………………………………………………

   …………………………………………………………………………………

3. How can you improve the performance of twisted pair cables?

   …………………………………………………………………………………

   …………………………………………………………………………………

4. Describe the principal of optical fiber and its advantages and disadvantages?

   …………………………………………………………………………………

   …………………………………………………………………………………

1.4 NETWORK TOPOLOGIES

Network Topology is the study of the arrangement or mapping of the elements (links, nodes, etc.) of a network interconnection between the nodes. It also determines the strategy for physically expanding the network, in future. Topologies can be physical or logical. Physical Topology means the physical design of a network including the devices, location and cable installation. Logical Topology refers to the fact that how data actually transfers in a network as opposed to its design.

There are different types of the topologies like bus, ring, tree, mesh etc. However, we will discuss only the first three to introduce you to the concepts.

1.4.1 Bus Topology

Bus topology is a single common communication to which all the computers are connected. It has a single length of cable with a terminator at each end as shown in the Figure 1.7. It is a passive topology which means only one computer at a time can send a message. Hence, the number of computers attached to a bus network can significantly affect the speed of the network. A computer must wait until the bus is free before it can transmit. Each node is connected to others nodes. The network operating system keeps track of a unique address of each node and manages the flow of data between machines.

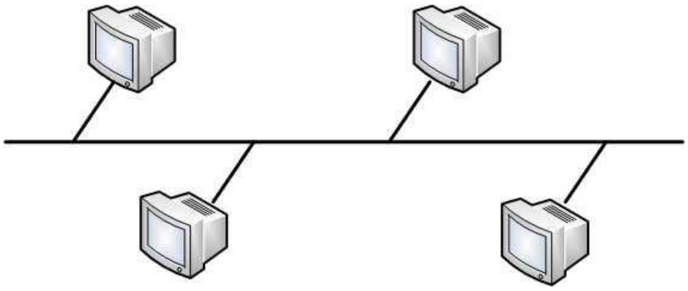


Figure 1.7: Bus topology

The bus topology is the simplest and most widely used with local area network design. The computers on the bus keep on listening. When they hear data that belongs to them, they receive. When one device on the network wants to send a broadcast message to another device on the network, it first makes sure no one else on the bus is transmitting, and then it sends information out on the media. All other devices on the network see it, but only the intended recipient accepts and processes it. This is accomplished by using data frames which contain source and destination addresses.

Advantages

a) It is simple, reliable, and easy to be used in a small sized local area network.

b) It requires least amount of cable to connect computers together and is therefore less expensive than other cabling arrangements.

c) It is easy to implement and extend using connectors.

d) If one computer on the bus fails, it does not affect the rest of the traffic on the bus.

Disadvantages

a) In this topology, no two computers can transmit data at the same time.

b) It does not cope well with heavy load which can slow down a bus considerably.

c) Performance degrades as additional computers are added.

d) Terminators are required at both ends of the cable.

1.4.2 Ring Topology

Ring topology is also known as circular topology. This layout is similar to the linear bus, except that the nodes are connected in a circle as shown in Figure 8. In this topology, each node is connected to two and only two neighboring nodes. The ring does not have an end. It is made of short segments that connect one PC to the next PC and so on Data is accepted from one of the neighboring nodes and is transmitted onwards to another node .Therefore data travels in only direction from node to node around the rings. Since, each computer retransmits what it receives, a ring is an active network and is not subject to the signal loss problems. There is no termination because there is no end to the ring.

This type of topology can be found in peer-to-peer networks, in which each machine manages both information processing and the distribution of data files. Examples of such topology:

1) IBM Token Ring
2) Fiber Distributed Data Interface (FDDI)

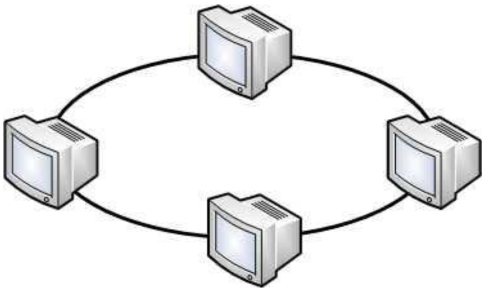


Figure 1.8: Ring topology

Advantages

a) It is an orderly network where every device has access to the token (control signal) and the opportunity to transmit – because every computer is given equal access to the token, no computer can monopolize the network.

b) It performs better than a star topology under heavy network load.

c) It can create much larger network using Token Ring.

d) It does not require network server to manage the connectivity between the computers.

Disadvantages

a) Network adapter cards and Multi Access Units used in this topology are much more expensive than Ethernet cards and hubs used in bus topology.

b) It is much slower than an Ethernet network under normal load.

c) It is difficult to troubleshoot.

d) One malfunctioning node or bad port in the Multi Access Units can create problems for the entire network

1.4.3 Star Topology

In star topology, each computer on a network communicates with a central hub (also called as a concentrator) that re-sends the message either to all the computers or only to the destination computer. A hub expands one network connection into many. For example, a four-port hub connects up to four machines. A single hub is sufficient for a small network; however large networks require multiple hubs. But, it increases hardware and cabling costs.

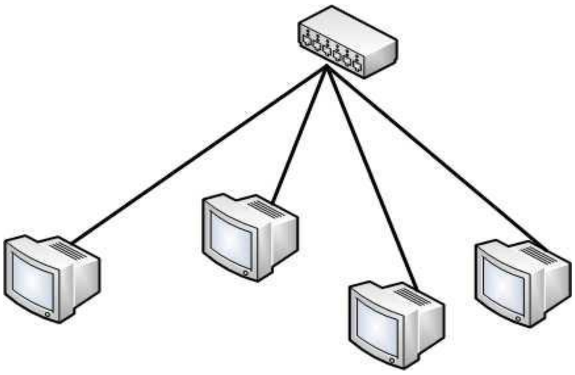


Figure 1.9: Star Topology

Advantages

a) It is more reliable (if one connection fails, it does not affect others) –The centre of a star network is a good place to diagnose network faults and if one computer fails whole network is not disturbed. Hub detects the fault and isolates the faulty computer.

b) It is easy to replace, install or remove hosts or other devices, problem can be easily detected-It is easier to modify or add a new computer without disturbing the rest of the network by simply running a new line from the computer to the central location and plugging it to the hub.

c) Use of multiple cables types in a same network with a hub.

d) It has good performance

Disadvantages

a) It is expensive to install as it requires more cable, it costs more to cable a star network because all network cables must be pulled to one central point, requiring more cable length than other networking topologies.

b) Central node dependency, if central hub fails, the whole network fails to operate.

c) Many star networks require a device at the central point to rebroadcast or switch the network traffic.

1.5 NETWORK CLASSIFICATION

There are mainly three types of networks:

1) LAN (Local Area Network)

2) MAN (Metropolitan Area Network)

3) WAN (Wide Area Network)

1.5.1 Local Area Network (LAN)

LAN (Figure 1.10) is a group of computers located in the same room, on the same floor or in the same building that are connected to form a single network as to share resources such as disk drives, printers, data, CPU, fax/modem, applications etc.

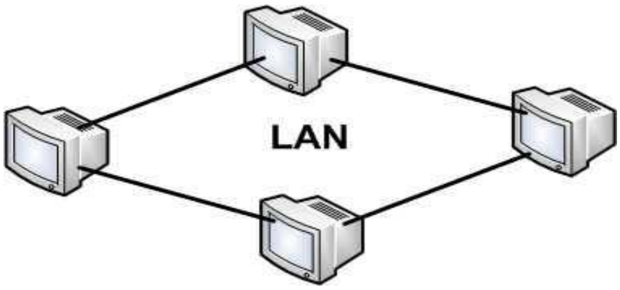


Figure 1.10: LAN

LAN is generally limited to specific geographical area less than 2 Km., supporting high speed networks. A wide variety of LANs have been built and installed, but a few types have more recently become dominant. The most widely used LAN system is the Ethernet system based on the bus topology.

Intermediate nodes (i.e., repeaters, bridges and switches discussed in section 1.7) allow to be connected together to from larger LANs. A LAN may also be connected to another LAN or to WANs and MANs using a “Router” device.

In general, there are five components of a LAN:

1) Network devices such as Workstations, printers, file servers which are normally accessed by all other computers.
2) Network Communication Devices i.e., devices such as hubs, routers, switches etc. that are used for network connectivity.
3) Network Interface Cards (NICs) for each network device required to access the network. It is the interface between the machine and the physical network.
4) Cable as a physical transmission medium. However, present day LAN may not require the physical transmission media. It may be a Wireless LAN. (Please refer to further readings for more details on wireless LANs)
5) Network Operating System –software applications required to control the use of network operation and administration.

Characteristics of LAN

- It connects computers in a single building, block or campus, i.e. they work in a restricted geographical area.
- LANs are private networks, not subject to tariffs or other regulatory controls. For the Wireless LANs there are additional regulations in several countries.
- LANs operate at relatively high speed when compared to the typical WAN (.2 to 100 MB /sec).
- There are different types of Media Access Control methods in a LAN, the prominent ones are Bus based Ethernet, Token ring.

Advantages of LAN

- It allows sharing of expensive resources such as Laser printers, software and mass storage devices among a number of computers.
- LAN allows for high-speed exchange of essential information.
- It contributes to increased productivity. A LAN installation should be studied closely in the context of its proposed contribution to the long range interest of the organization.

Disadvantage of LAN

Some type of security system must be implemented if it is important to protect confidential data. The security may be further low if it is a wireless LAN.

1.5.2 Metropolitan Area Network (MAN)

Metropolitan area networks, or MANs, are large computer network that spans a metropolitan area or campus. Its geographic scope falls between a WAN and LAN. They typically use wireless infrastructure or Optical fiber connections to link their sites.

A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities or privately owned. They will often provide means for internetworking of local networks. Metropolitan area networks can span up to 50km, devices used are modem and wire/cable.

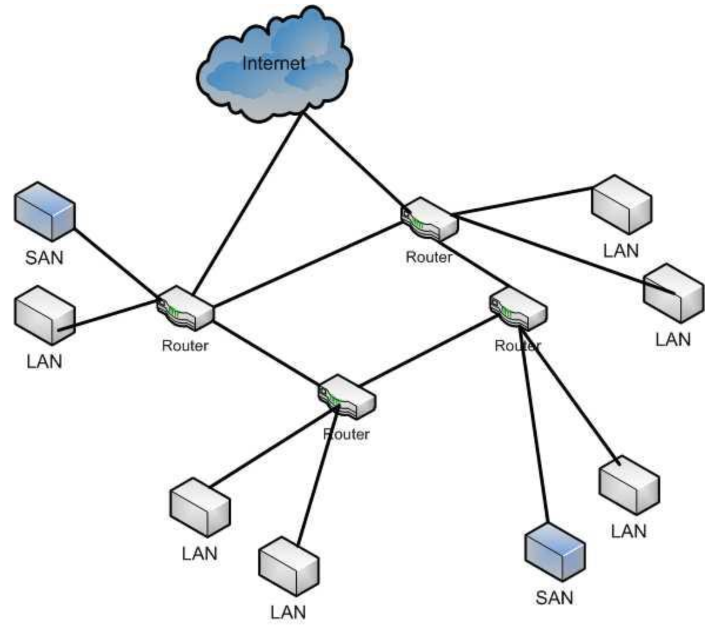


Figure 1.11: MAN

MANs provide Internet connectivity for LANs in a metropolitan region, and connect them to wider area networks like the Internet.

1) The network size falls intermediate between LAN and WAN. A MAN typically covers an area of between 5 and 50 km diameter. Many MANs cover an area the size of a city, although in some cases MANs may be as small as a group of buildings or as large as the North of Scotland.

2) A MAN often acts as a high speed network to allow sharing of regional resources. It is also frequently used to provide a shared connection to other networks using a link to a WAN.

Characteristics of MAN

1) It generally covers towns and cities (50 kms)

2) It is developed in 1980s.

3) Communication medium used for MAN are optical fiber cables, however it may use other media too.

4) Data rates adequate for distributed computing applications.

1.5.3 Wide Area Network (WAN)

Wide Area Network (Figure 1.12) is a network system connecting cities, countries or continents, a network that uses routers and public communications links. The largest and most well-known example of a WAN is the Internet.

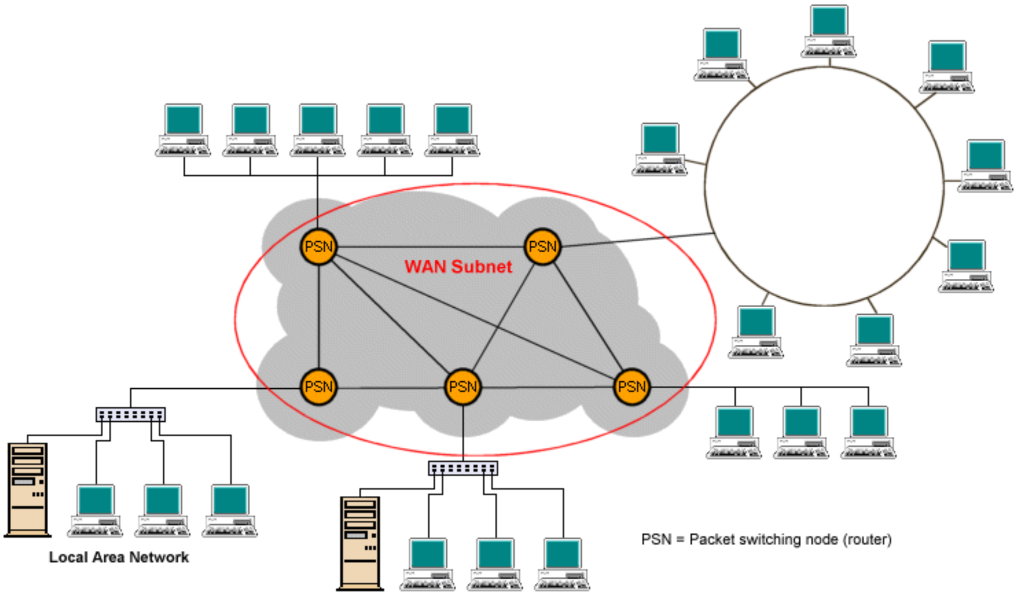


Figure 1.12: WAN

WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet. WANs are often built using leased lines. At each end of the leased line, a router connects to the LAN on one side and a hub within the WAN on the other. Leased lines can be very expensive. Instead of using leased lines, WANs can also be built around public network or Internet.

Virtual Private Network (VPN): Consider a situation when you have a secure office LAN which contains some important update of your company products. You are out of the country for a business trip and want to see that information. What your company needs is a VPN. A VPN may be defined as the secure way of connecting to your private LAN (such as your company network) from a remote location using the Internet or any other unsecure network. In such a case, the data that is to be transmitted over the unsecure network is encrypted. In addition, VPNs have a proper mechanism for authenticating the user.

Characteristics of WAN

1) It generally covers large distances (states, countries, continents).

2) Communication medium used are satellite, public telephone networks which are connected by routers.

3) Routers forward packets from one to another on a route from the sender to the receiver.

Table 1.1 compares the three technologies :

Table 1.1: Difference between LAN, WAN and MAN

Characteristics	**LAN**	**MAN**	**WAN**
Full form	It stands for local area network.	It stands for metropolitan area network.	It stands for wide area network.
Cost	Less Costly	More Costly	Costliest
Speed (in general)(the speed is moving beyond the limit)	Upto 10-1 Gbps	5- 10 Mbps and beyond	256 Kbps to 2 Mbps and beyond
Range	1 Km	Upto 50 Kms	Whole earth (20.000 Km in each direction)
Topology	Bus and Ring	Distributed Queue Dual Bus [DQDB]	ATM, Frame Relay, Sonet
Location of computers connected in the system	Computers are located within the same building.	Computers are located in the city and are connected using modems or telephone lines so that they can be easily connected with each other.	Computers are distributed all over the country or the continent. The connection is made via satellite communication link or via internet.
Examples	LAN's example can be an office whose different departments such as personnel, accounting etc. are located in the same building and connected via bus topology using Ethernet cards.	Example of MAN is bank whose different branches in a city like Delhi are connected using public telephone exchange and the system are connected with each other using LAN within each branch and different branches are connected using modem and bridges.	WAN's example is the connection of various branches of MNC such as Proctor & Gamble. These branches are linked using microwave satellite communication system or internet connection. Each branch has its own LAN circuit. But the different LAN's in various branches are communicating with head office using WAN link.

1.6 REFERENCE MODELS

One of the most difficult software to be developed is the networking software. Reference models were designed to standardize the layer of functions and activities. The following section describes one of the most important reference models used in Computer Networks.

OSI (Open System Interconnection) Model

The OSI model is an abstract description for layered communications and computer network protocol design open system means that it can communicate with any other system that follows the specified standards, formats and semantics. **Protocols** give the rules that specify how the different parties may communicate.

In its most basic form, it divides network architecture into seven layers which from top to bottom are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers. It is therefore often referred to as the **OSI Seven Layer Model (Figure 1.13)**.

A layer is a collection of conceptually similar functions that provide services to the layer above it and receives service from the layer below it. On each layer an *instance* provides services to the instances at the layer above and requests service from the layer below. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of the path. Any two instances at one layer are connected by a horizontal protocol connection on that layer.

The following are the layers of OSI model:

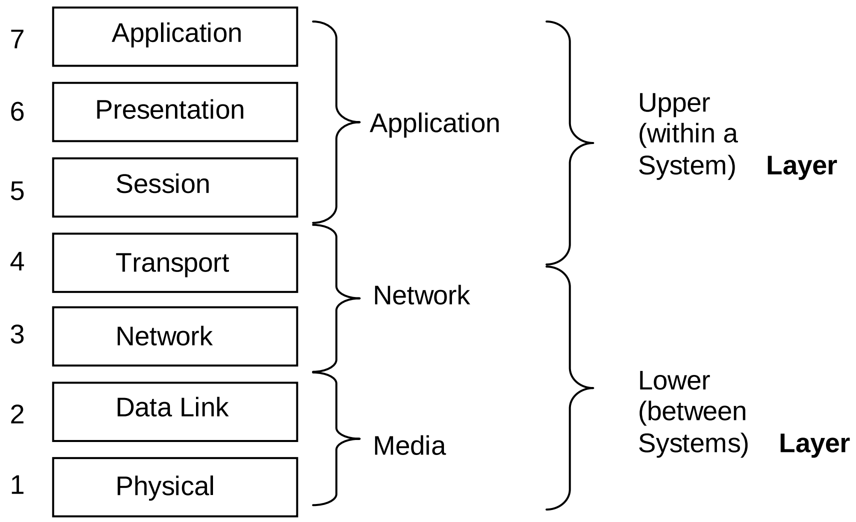


Figure 1.13: OSI Model

In transmission side data flows from layer 7 to layer 1, then to cabling or suitable medium. When data reaches the reception side, it flows from layer 1 to layer 7.

Application Layer: This layer is the layer for user interaction. We must have application software for dealing with the data.

Presentation Layer: It converts the data into suitable format. It does tasks like compression, decompression, encryption and decryption.

Session Layer: This layer manages connections between different application layers.

Transport Layer: This layer converts data into segments and re-assembles the data stream. TCP and UDP are the protocols used in this layer. In this layer, data is converted into so called segments.

Network Layer: This layer translates logical address into physical address. This layer also fixes the route for data path. Router works in this layer. In this layer data is called a packet.

Data-Link Layer: This layer provides physical identification of a device using Media Access Control Address. It adds source and destination address to packets and convert them into frames. This is the layer that provides error free transmission.

Physical Layer: This layer provides the functional requirements for activating a physical link. In this layer, data is carried from one device to another.

Now, we can better understand the OSI layer with an example. Consider that you have to send a word document to a different network or through internet. The following are the process that will take place:

1. In the APPLICATION LAYER, the user can edit the file by using application software like a word processor.

2. In the PRESENTATION LAYER, user can compress the word file by using WINRAR or WINZIP and convert the data into different format for example.zip or .rar. You can also convert the word document into different formats.
3. In the SESSION LAYER, the particular file has to be integrated with browser for attaching it to email or likewise clients.
4. In the TRANSPORT LAYER, data is converted to segments. Source IP and destination IP are added to each packet. Frame checks and parity bits are also added in this layer.
5. In the NETWORK LAYER, the data is handed over to a router. The router calculates the best path for data transmission
6. In the DATA-LINK LAYER, transmission errors are handled and also flow of data is regulated so that receivers are not swamped by fast senders.
7. In the PHYSICAL LAYER, frames are transmitted as bits through media such as Optical fibre.

1.7 NETWORKING DEVICES

For creating a network, you need certain basic devices. This section details some of these basic devices which are used to form a network. Network Interface cards, Hubs, bridges, repeaters, and routers are the devices that let you connect one or more computers to other computers, networked devices, or to other networks. Each has two or more connectors called ports (this term presently is used in the context of hardware) into which you plug in the cables to make the connection. Let us discuss each of these communication devices in detail.

1.7.1 Network Interface Cards

The network interface card (NIC) provides the physical connection between the network and the computer. Most NICs are internal, with the card fitting into an expansion slot inside the computer. Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for fast transfer of data. The most common network interface connection today is Ethernet cards. **Ethernet cards** Ethernet cards that contain connections for twisted pair cables have a RJ-45 connection. The Ethernet card is sometimes also called as network adapter card. Each for the Ethernet card is identified by a unique number called the Media Access Control (MAC) address. Your mobile phone on which you use internet, generally has a MAC address.

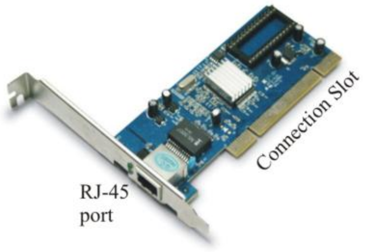


Figure 1.14: Network Interface Card

1.7.2 Modem

Modem is an acronym for modulator demodulator. The meaning of the word modulator is to change and the meaning of the word demodulator is to restore to an original condition. A modem is a communication device that converts (i.e., modulates) binary signal into analog signals for transmission over telephone lines and converts (i.e., demodulates) these analog signals back into binary form at the receiving end.

Figure 1.15 shows the data transmission through modem

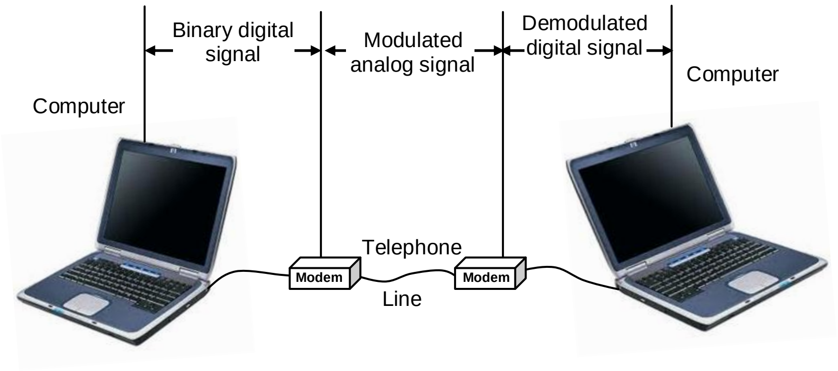


Figure 1.15: Data transmission through a modem

You can use a modem to send data and files to other computer users using standard telephone lines. You can transfer data, exchange electronic files, and even carry on a typed conversation in real time.

Modems are of two types: Internal and External. Internal modems are hardware cards and External modems, are kept outside of your computer, connected either by a USB or Serial Port. Internal modems are good for general usage, as they take up less desk space, and do not require a power supply, and for most purposes, internal modems work fine. External modems tend to be slightly more expensive than internal modems. Many experts consider them superior because they contain lights which indicate how the modem is functioning. In addition, they can easily be moved from one computer to another. However, they do use up one COM port.

External modem

Internal modem

Figure 1.16: Modems

1.7.3 Repeaters

When a signal travels a network cable (or any other medium of transmission), they lose strength, degrade and become distorted in a process that is called attenuation A repeater is a device that electrically amplifies the signal it receives and re-broadcasts it (Figure 1.17). They are used when the total length of your network cable exceeds the standards set for the type of cable being used.

A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling. If a cable is long enough, the attenuation will finally make a signal unrecognizable by the receiver.

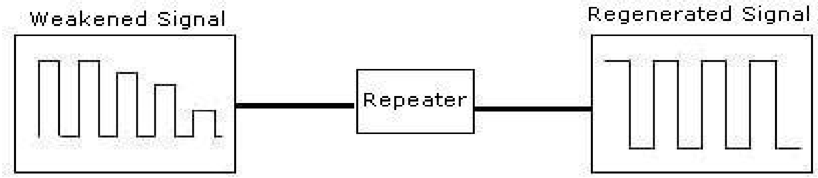


Figure 1.17: Repeater

1.7.4 Bridge

Like a repeater, a bridge can join several LANs. However, a bridge can also divide a network to isolate traffic problems. For example, if the volume of traffic from one or two computers or a single department is flooding the network with data and slowing down entire operation, a bridge can isolate those computers or that department. A bridge (Figure 1.18) is used to connect two segment i.e., segment 1 (LAN 1) and segment 2 (LAN 2). Each segment can have several computer attached to it.

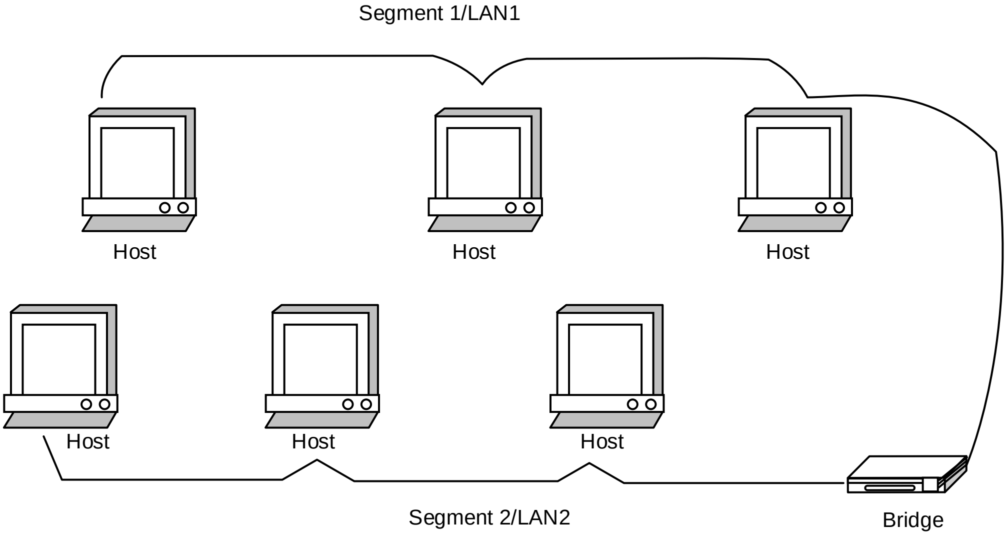


Figure 1.18: Bridge

1.7.5 Hub

A hub sends any data packet coming from one port to all other ports. It is up to the receiving computer to decide if the packet is for it. Typically used to connect segments of a local area network (LAN), a hub contains multiple ports. You can imagine packets going through a hub as messages going into a mailing list. The mail is sent out to everyone and it is up to the receiving party to decide if it is of interest. The biggest problem with hubs is their simplicity. Since every packet is sent out to every computer on the network, there is a lot of wasted transmission. This means that the network can easily become bogged down.

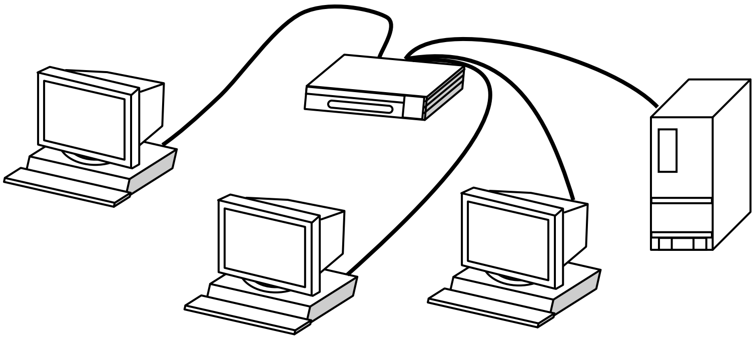


Figure 1.19: Hub

Hubs are typically used on small networks where the amount of data going across the network is never very high. A hub is typically the least expensive, least intelligent, and least complicated of the hub, router and switches. Every computer connected to the hub "sees" everything that every other computer on the hub sees.

1.7.6 Switches

A switch does essentially what a hub does but more efficiently. By paying attention to the traffic that comes across it, it can "learn" where particular addresses are. For example, if it sees traffic from machine A coming in on port 2, it now knows that machine A is connected to that port and that traffic to machine A needs to only be sent to that port and not any of the others. The net result of using a switch over a hub is that most of the network traffic only goes where it needs to rather than to every port. On busy networks this can make the network significantly faster.

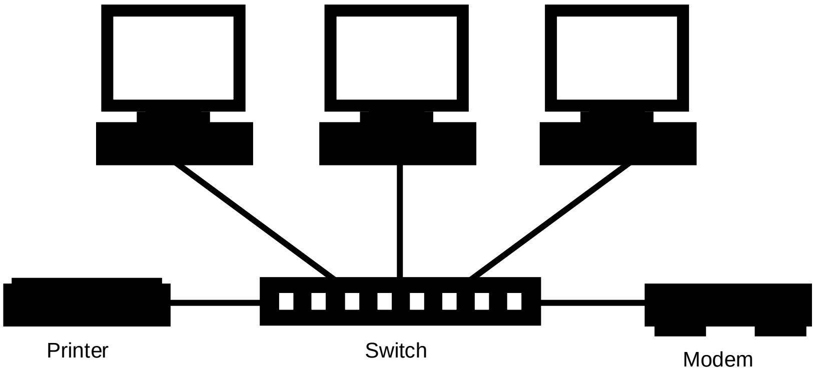


Figure 1.20: Switch

A switch (or Switching Hub) is a device that can segment a larger local area network to reduce the traffic load. One should implement a switch when you have a network with 20 or more users that have bogged down the network by excess traffic. It splits the network into two or more segments with devices that normally talk with each other. Conceptually – switching takes data from one interface and delivers it to another interface.

1.7.7 Router

A router translates information from one network to another; it is similar to an intelligent bridge. Router selects the best path to route a message, based on the destination address and origin. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along shortcuts. Routers can even "listen" to the entire network to determine which sections are busiest—they can then redirect data around those sections until they are removed.

If you have a LAN that you want to connect to the internet, you will need to purchase a router. In this case, the router serves as the translator between the information on your LAN and the internet. It also determines the best route to send the data over the internet. Routers maintain a map of the physical networks on a Internet (network) and forward data received from one physical network to other physical networks.

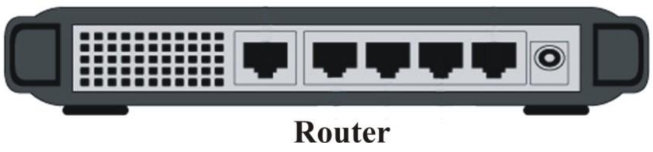


Figure 1.21 : Router

1.7.8 Gateway

If you are connected to the internet, you have to enter through a Gateway. A Gateway connects your smaller network to the internet. A gateway passes information from one network to another network as your information travels across the internet.

Gateway Interconnects networks at higher layers than bridges or routers. A gateway usually supports address mapping from one network to another, and may also provide transformation of data between the environments to support end to end application connectivity. Gateway typically limits the interconnectivity of two networks to a subset of the application protocols supported on either one.

Routers exemplify special cases of gateways. Gateway, also called protocol converters, can operate at any layer of the networking model. The job of a gateway is much more complex than that of a router or a switch. Typically, a gateway must convert one protocol into another.

The main function of a gateway is to convert protocols among communications networks. A router by itself transfers, accepts and relays packets only across networks using similar protocol. A gateway, on the other hand, accepts data formatted for one protocol and convert it to data formatted for another protocol before forwarding it. A gateway can be implemented in hardware, software or both, but they are usually implemented by the software installed within a router. A gateway must understand the protocols used by each network linked into the router. Gateways are slower than bridges, switches and (non- gateway) routers.

The computers of Internet users and the computers that serve pages to users are host nodes, while the nodes that connect the network in between are gateways. For example, the computers that control traffic between company networks or the computers used by internet service providers (ISPs) to connect users to the internet are gateway nodes.

Check Your Progress 2

1) Identify the characteristics of bus, ring and star topologies and write the best characteristic that you think while designing a topology.

……………………………………………………………………………………

……………………………………………………………………………………

2) Differentiate amongst LAN, MAN and WAN in terms of their coverage area.

……………………………………………………………………………………

……………………………………………………………………………………

3) Identify the examples of networks around you and classify them in terms of LAN, MAN and WAN.

……………………………………………………………………………………

……………………………………………………………………………………

4) Differentiate between a bridge and a router.

……………………………………………………………………………………

……………………………………………………………………………………

5) Explain the function of hub and where should we use this communication device?

……………………………………………………………………………………

……………………………………………………………………………………

6) What is the function of gateway?

……………………………………………………………………………………

……………………………………………………………………………………

1.8 INTERNET AND ITS SOFTWARE COMPONENTS

After through some of the basic networking concepts, let us now look into some more concepts relating to one of the major application of networks the Internet. You have been introduced to internet in section 1.2.2. Let us once again sketch some of the basic points on Internet.

- Internet is a global connection of networks. But, how are these computer connected? The Internet is basically built up of multiple smaller networks called the subnets. Each computer systems on a subnet must have a *unique address*. All these subnets are connected together with network devices called routers, and each subnet may also contain its own subnets.
- Figure 1.22 is a top level view of the structure of the Internet as a cloud of many routers that are connected to each other. You may be able to connect to any of the search engines that allows you to locate information on Internet or any of the web servers like IGNOU web server through many alternative routes. A client may be a part of LAN, WAN or wireless network, it does not matter. Everything is almost in the Internet cloud -why? Because all these networks use one common protocol for reliable data transfer, so they speak common language and communicate irrespective of physical differences. This basic communication protocol on Internet is the Transmission Control Protocol/ Internet Protocol (TCP/IP). This protocol ensures reliable delivery of information from one source identified by a unique IP address to a destination also identified by a unique IP address. Please note that the source and destination computer may either be local or remote computer, depending on the destination location. But what are these IP addresses?

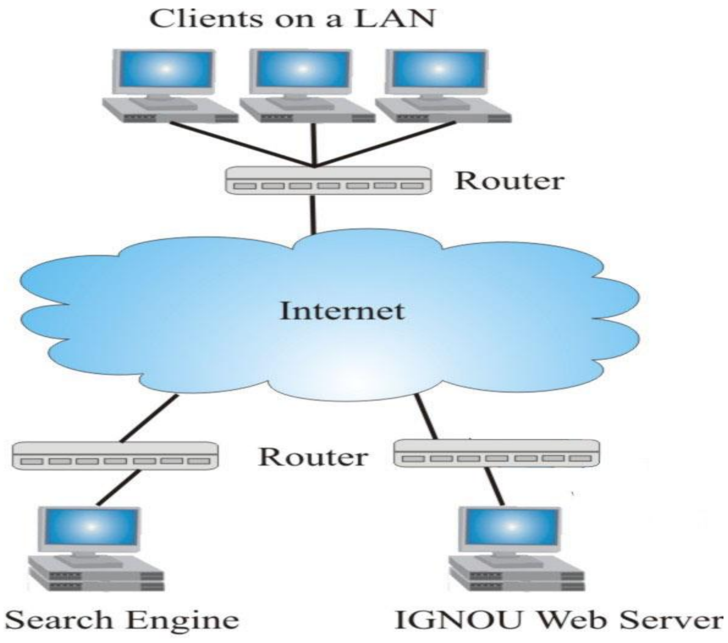


Figure 1.22 : Structure of Internet

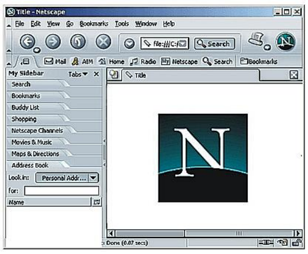
- To connect to a physical network, all devices irrespective of being wired or wireless uses an interface card. An interface card may have its own unique physical address. However, you cannot locate a device just by its unique physical address, as these addresses do not provide any indication about the location of the device. Thus, you require a protocol that uniquely identifies a device on the Internet and Internet protocol version 6 (IPV6) which is beyond the scope of this unit.

- TCP and IP (TCP/IP) are the two core protocols of the Internet Protocol suite. The TCP primarily provides the reliable delivery of stream of bytes from a computer or a program to another computer or a program. It breaks the data stream into packets at the source and makes sure that all the packets are assembled orderly at the destination. The IP protocol on the other hand identifies the location of source and the destination. Any computer on Internet is identified by its unique IP address. Currently two standard versions of IP are available viz. Internet Protocol Version 4 (IPv4) which is currently being used on most of the Internet. An IPv4 address is a 32 bit address. IPv6 has not been discussed in this Unit.

- Using the TCP/IP as the basic protocol Internet offers many services and application to it users like work wide web, Email, Chat, Social networking, collaboration etc

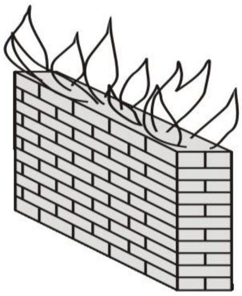
- WWW is one of the major applications of Internet and is based on the concept of Hypertext that is hot links to a document that may reside on any website. It is a global infrastructure of connected documents.

- Following are some of the major Software Components required to access Internet:



  - The first **software** for internet access is the Operating system. An operating system must be installed properly on your system (so that it can handle the driver requirements of the hardware components).

  - **Internet Browser:** Browser is software that allows the user to access and read information on the World Wide Web. Internet Explorer, Mozilla, Netscape are the best-known browsers. SpaceTime 3D is new three-dimensional browser. Only browser is sufficient for working with the Internet viz., the browser software that should be loaded on all the clients. In fact, the browser is one of the very intelligent software that contributed to the growth of World Wide Web. A browser converts the standard Hyper Text Markup Language (HTML) web pages to a very sophisticated display with colours and pictures.



Firewall

  - **Firewall:** Internet has many security problems like hacking, Trojan Horse, Virus, etc. There are various tools to provide protection against unwanted access of your computer by anyone else, but the most popular among all security measures is the firewall. Firewall is software that works on some set of rules and instructions given by you. A firewall helps to keep your computer more secure. It restricts information that comes to your computer from other computers, giving you more control over the data on your computer and providing a line of defense against people or programs (including viruses and worms) that try to connect to your computer without invitation.

  - **TCP/IP protocol:** This is the group of protocols that define the Internet and communication method used by it. Let us discuss it in more details :

TCP/IP Stack

TCP/IP was originally designed for the UNIX operating system; however, TCP/IP software is now available for every major operating system. In order to be compatible to the Internet, the computer must have TCP/IP compatible software. The major advantage of Internet is information sharing. Since in computers, bits and bytes are basic building blocks of information. Thus, one of the key aspects in network of many computers is to move bits between two specific computers. For such a communication, we require the address of the destination and a safe mean of moving data in the form of electronic signals. As far as safe movement of data is concerned, there exists a set of rules, which governs the sending, and receiving of data on the Internet.

A stack of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol) implements these rules. Its name reflects names of only two protocols called TCP and IP. For sending large block of text/data to another machine, TCP divides the data into little data packets. It also adds special information e.g., the packet position, error correction code etc. to make sure that packets at the destination can be reassembled correctly and without any damage to data. The role of IP here is to put destination-addressing information on such packets. *On Internet, it is not necessary that all the packets will follow the same path from source to destination*. A router tries to load balance various paths that exist on networks. Other gateways allow different electronic networks to talk to Internet that uses TCP/IP.

The Internet layer is an important layer in the protocol suite. At this layer, TCP/IP supports Internet Protocol (IP). This layer is responsible for the format of datagram or a packet as defined by IP and routing and forwarding a datagram or packet to the next hop (hop is a term that can be used to represent any computing device on Internet like; router, gateway, computer etc. A hop is the trip from one device to the next.) The primary goal of the Internet is to provide an abstract view of the complexities involved in it. Internet must appear as single network of computers. At the same time network administrators or users must be free to choose hardware or various internetworking technologies like Ethernet, Token ring etc. Different networking technologies have different physical addressing mechanisms. Therefore, identifying a computer on Internet is a challenge. To have uniform addressing for computers over the Internet, IP defines an IP address, which is a logical address. IP address is a 32 bits number, can be represented in decimal e.g., 192.168.32.10. Now, when a computer wants to communicate with another computer on the Internet, it can use logical address and is not bothered with the physical address of the destination and hence the format and size of data packet. IP address is a basic address used by the lower architecture of Internet. It is important for you to know that, any address you type as web address or email address actually gets converted into the equivalent IP address of a machine or computer where the server or resource is available. Web address or email addresses are used for ease and convenience of human beings otherwise; it is just a burden for network.

TCP/IP Model

Just like the OSI model, the TCP/IP model has many layers which are described below:

Host to Host Network: In fact TCP/IP model does not specify this layer. But it basically combines functionally of physical and data link layers. Starting at the bottom, the Physical layer is what deals with hardware (wires, cables, satellite links, NICs, etc.). Utilizing the existing Physical layer, TCP/IP does not define its own, thus letting the layer be compatible with all network suites. This layer also encodes and transmits data over network communications media in the form of bits which are received by the Physical layer of the destination device. Often combined with this layer is the Data link layer which is responsible for moving packets from the network layer onto different hosts. Depending on the connection type, IP packets are transmitted using various methods. Dial-up modems transmit IP packets using PPP while broadband users transmit using PPoE.

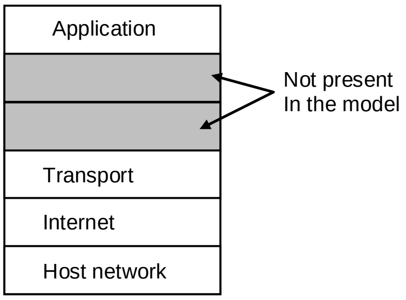


Figure 1.23 : TCP/IP Model

Internet Layer: This layer routes and delivers data across similar networks or completely different networks. The Network layer is responsible for end to end packet delivery while maintaining routing, flow control, and error control functions. An example of this layer is the Internet Protocol (IP) or the Internet Protocol Security (IPSec).

Transport Layer: The Network layer can be thought of the actual vehicle which transports information. This layer categorizes end to end message transmissions or connecting applications as either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). TCP is a connection-oriented protocol which is considered to provide a reliable byte stream. Some characteristics of TCP are traffic congestion control, data arrives in order, data has minimal error, and duplicate data is discarded.

The top layer of the TCP/IP model is the Application layer which is used for network communication. Ports are used by programs to transfer data through this layer. For example, the File Transfer Protocol uses port 21 by default while the Hypertext Transfer Protocol uses port 80.

TCP/IP has many benefits. TCP/IP enables cross-platform networking which is useful in this day-in-age. This suite also has superior failure recovery and the ability to add networks without interrupting existing services. The reliability of TCP/IP is also a huge benefit to using this protocol. The fact that if one part of the network goes down, other parts are still able to function is what has set TCP/IP above other networking protocols. TCP/IP is also easily expandable which allows for the unprecedented rate of growth which the Internet possesses.

1.9 INTERNET ADDRESSES

We can classify the computers connected with Internet in two categories, servers and clients. A server is a computer with the capacity to provide connectivity and sharing to multiple personal computers or clients (any computing device you use to access the Internet), which is specifically set up to serve its files to client computers. The files that a server makes available to your computer can be web pages, videos, sounds, images, etc. A web server normally has:

- A high end computer with web server software. The three most popular web server software are:
  - Apache HTTP Server, available in public domain
  - Microsoft Internet Information Services (IIS)
  - Sun Java System Web Server
- A very good Internet connection speed, so that it can support multiple simultaneous users.
- Its own URL and IP address. (What is a URL? URL - Uniform Resource Locator. URL is theglobal address of a document or resource on the WWW)

For your home computer to be able to receive files or any data from a server, your computer must request this information. This happens when you enter an URL in your browser or when you receive e-mail. When we work on Internet we come across different types of addresses used for different purposes, like; web address, IP address, email address. Each one has a special syntax, and meaning. It is important for you to know about these addresses, before you start working on Internet.

1.9.1 IP Addresses

Figure 1.23 shows an IPv4 address:

IP address: 192.168.1.97 in various forms:

Decimal	192		168		1		97	
Hexadecimal	C	0	A	8	0	1	6	1
Binary	1 1 0 0	0 0 0 0	1 0 1 0	1 0 0 0	0 0 0 0	0 0 0 1	0 1 1 0	0 0 0 1

Figure 1.23: IP Address

IPv4 address is a series of four numbers separated by dots (.). The four numbers ranges between 0 and 255. So IPv4 address takes only 4-bytes (or 32-bits) of computer memory. Not all the IPv4 addresses may be used to identify a computer. Some addresses of IPv4 are not used at all due to certain restrictions. In addition, some addresses are reserved, for example; the IP address 255.255.255.255 is used for broadcasts.

Every device, computer, printer or peripheral connected to a TCP/IP network must have its own IP address. Each 32 bit IP address consists of two components:

- Network Identifier (Net ID) – which identifies one of the Networks that is a part of Internet.
- Device Identifier (Device ID) – which identifies a specific device within the identified Net-ID.

A Net ID may be of 8 to 24 bits long. By using a subnet mask in combination with their own IP address, you can determine the destination address of the devices is remote or local. For example, consider the IP address 192.168.1.35, having 24 bits Net ID. The remaining 8 bits of this address specifies the device ID. The subnet mask for this network should be 255.255.255.0. This subnet mask is used to identify the IP address of the network.

Now, consider a situation in your office, you want to create a small network, but your network service provider has given you only one IP address? Fortunately, there are IP addresses that have been kept for private network. These addresses are not globally allotted to any organisation but are addresses with in your private network. To connect your private network to the Internet, you are required either to use a network address translator gateway, or a proxy server. Please refer to further readings for more details on these networks. The IP range that is allocated for such non-routable addresses are:

IP Address	Subnet Mask	Number of IP addresses (some what equivalent to maximum possible number of Computers/ network devices
10.0.0.0 – 10.255.255.255	255.0.0.0	16,777,216
172.16.0.0 – 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0 – 192.168.255.255	255.255.0.0	65,536

The subnet mask is similar to an IP address - it is also a 4-byte (or 32-bits) field and can be represented using dot notation. In binary, it always comprise a series of ones, followed by sequence of zeros. The total number of bits is 32, but the number of ones and zeros determines the nature of the mask. By comparing any IP address with a given mask, you can split addresses into two parts, a network ID and a device ID. The following example explains this concept in more details.

Suppose your computer has an IP address of 193.168.1.35 and you want to access a location 193.168.1.56, as your subnet mask is 255.255.255.0, it will give you following answers:

Host (you):	193.168.1.35
Subnet Mask	255.255.255.0
Result:	193.168.1.0
Accessed Location	193.168.1.56
Subnet Mask	255.255.255.0
Result:	193.168.1.0

Since, the Result of both the operation points to same Net ID, therefore, you can conclude that the referred destination IP address is local.

Now, suppose your computer has an IP address of 191.168.1.35 and your NetID is 16 bit long. Suppose you want o access a location 190.168.1.35. Since, you have 16 bit NetID, therefore, your network subnet mask will be 255.255.0.0, it will give you following answers:

Host (you):	191.168.1.35
Subnet Mask	255.255.0.0
Result:	191.168.0.0
Accessed Location	190.168.1.35
Subnet Mask	255.255.0.0
Result:	190.168.0.0

Sub-netting is based on CIDR (Classless Inter-Domain Routing) concept. It is used in routing between networks both locally and

Since, the Result of both the operation points to different Net ID, therefore, you can conclude that the referred destination IP address is remote.

By comparing the source network ID with the IP address of the source and the network ID of the destination IP address, you can easily determine if the destination is within the same subnet. A web page request, thus, can be identified as local page or a page from remote server. But, how do you find the location of the remote server? The answer to this question is beyond the scope of this unit. However, you should know that routers may be responsible in finding the final path to the remote server.

As the numbers of users are increasing, the IPv4 addresses will run short. Therefore, a 128 bit Internet Protocol Version 6 (IPv6) was designed which is at present actively being deployed on the Internet. This series can provide up to 3.4 X 10^{38} addresses. For more details on IPv6, please refer to Further Readings.

1.9.2 DNS and Web Addresses

An Internet or Web address is used to view a web page. When you are viewing a Web page, the web address of the page appears in the Address bar in the browser. In the previous section, you have gone through the concept of IP addresses. What do you think about the IP address? Are they not very cumbersome to remember? For example, to visit IGNOU website the address *www.ignou.ac.in* is far simpler than that of an IP address like 190.10.10.247. Obviously, what we want to use are simpler textual domain addresses instead of complex IP addresses. However, to enable the use of simple textual address, you will require a service that will map these text based names to respective IP addresses automatically. Such a service was designed in 1983 by the University of Wisconsin with the name Domain Name System (DNS).

In the present day, Internet, Domain Name System (DNS) should keep track of address of each computer or any other internet device and email addresses. The name servers translates the web address or email address to respective IP address. For example, the name server translates address like *www.ignou.ac.in* into a computer understandable IP address. It sounds simple, but remembers on Internet you are dealing with million of addresses and every day this list is increasing. All these computers have a unique address. Therefore, DNS follows a hierarchical naming scheme that is supported by distributed database system to ensure no duplicate names are issued at all. Figure 1.24 shows the hierarchical structure of domains names on Internet. For example, traversing the hierarchy from the top you can track down *ignou.ac.in* as:

First you can find the ***in*** (India) in the top level country domains. Within this domain find the ***ac*** (Academic) sub domain. Please note most of the Indian Universities will be in this sub-domain. Finally, in the ***ac*** you can find the entry for ***ignou.*** This entry should point to the IP address for the *ignou.ac.in* for the WWW as well as for the mail server. This is how the DNS finds the addresses, thus, is a very efficient system.

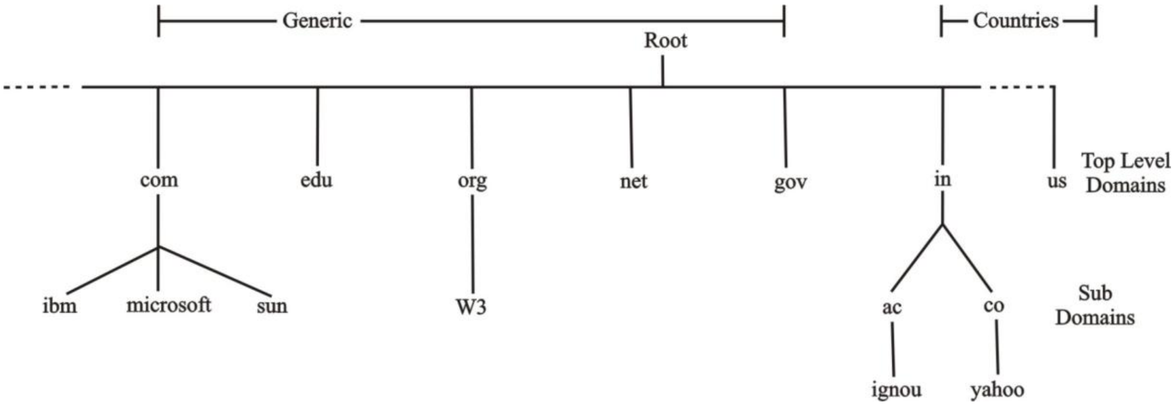


Figure 1.24: A sample portion of domain names on Internet

Thus, using the DNS you will be able to relate a given textual address to IP address. For converting domain name into IP address, it first accepts request from programs and other servers. After accepting the request, the name server can do the following:

- If it knows the IP address of requested domain, it will answer the request with an IP address of the requested domain.
- If it does not know the requested domain name, it will contact another name server and try to find the IP address.
- If the requested domain name is invalid or domain does not exist, it will return an error message.

But how can you name a web page on the Internet? To answer this question you may first identify that a web page actually is part of a website that may reside on a web server having a unique IP address. Thus, to identify a web page you need to identify –

- The protocol used to access that page.
- The server on which the website is located.
- The name of the page within that web site. Please note that simple web pages are stored as files.

Please note that a web page may be stored as a single or multiple files.

Thus, to identify a web page you will have an address like:

http://www.ignou.ac.in/students/result.html

- the address as above recognises the protocol http (Hyper Text Transfer Protocol) to access the page,
- the *www.ignou.ac.in* identifies the DNS name of IGNOUs WWW server, and
- the name of the page accessed by you is *result.html* which resides in the *students* folder within the website.

This address is called the URL. URL stands for Uniform Resource Locater.

You can now clearly see that a URL consists of three parts – the first part is used to tell the browser what kind of server it will connect to. In the example above, the browser will connect to a web server using Hypertext Transfer Protocol (HTTP). Other protocols that we can use in this field of an URL are FTP, smtp etc. the protocol is always followed by "**://**".

The second part of an URL is a fully Qualified Domain Name (www.ignou.ac.in). In an URL, the fully qualified domain name identifies the site running the server. Web servers use port 80 by default, but some servers has been set up to use other ports. For this, a URL can contain a port number following the domain name and separated from it by a colon (www.ignou.ac.in:80), it is optional to write a port number with domain name. If the URL contains no port number, the default port is used.

The range of Well Known Ports is in between 0–65535

The first two parts of an URL are used to identify the web server of the website. Each web server has a home page and a directory to store the entire document related to the web page like images, audio, video files.

The third component of URL is an optional pathname for a particular document itself. For example, the address *http://www.ignou.ac.in/students/result.html* specifies the file *result.html* i.e., in the directory *students* (/students/result.html) in the specified web server.

But how does this information exchange between the web client and web server is achieved? This whole communication is managed by a protocol called the Hyper Text Transfer Protocol (HTTP). However, the only protocol that works on Internet as told to you in the previous section was TCP/IP. So what is this HTTP? Please note HTTP can work only over a connection that is managed by TCP. Thus, it is a higher level protocol that uses the services of TCP.

URL - Uniform Resource Locator – identifies the GLOBAL address of a document or

HTTP specifies the list of actions that lead to transfer of a requested information exchange between a web client and web server. Whenever you wish to visit a web page on the internet, you request that page from a web server. When you type a URL into your browser (for example, "http://www.abc.com/"), your web browser requests the page (or file) named index.html from the web server and the web server sends the page back to the web browser. Let us identify these steps in more details:

1) As a first step you may put a URL like *http://www.abc.com/index.html* or equivalent Domain name www.abc.com as the address of the website that you want to access through your web browser.

2) The Web browser tries to resolve the IP address of the website www.abc.com by the information available in its own cache memory. If web server does not have the information about IP address stored in its cache, it requests the IP address from Domain Name System (DNS) servers. The DNS server tells the browser about the IP address of the website.

3) Once the web browser knows the IP address of the website, it then requests the web page (index.html page which is the home page in the present example) from the web server.

4) The web server responds by sending back the requested web page. If the requested page does not exist then it will send back the appropriate error message.

5) Your web browser receives the page from the web server and displays it as per the display requirements of the web page.

1.5.3 E-mail Addresses

As you have studied earlier that e-mail is one of the popular services increasingly being used by people in their daily life. The following can be a typical email address format on Internet for any e-mail service provider like, Gmail, Rediff, Yahoo, MSN, or any network (domain) name etc.

"My wife passed away months ago, but we are still in touch. Her e-mail is rupa@heaven.com"

username@subdomain.domain

The username in general is the name assigned or chosen during creation of an email account. Sub-domain are domain we have already discussed in above section, in case of private service provider it is generally its own name like *abc@yahoo.com, abc@yahoo.co.in, abc@gmail.com*, etc. On the Internet you can see both kind of domains non-Geographic and geographic domains. Lets take an example to better understand an e-mail address: In an e-mail address *"naveen@ignou.ac.in"*, naveen indicates the username, the sub-domain named IGNOU (Indira Gandhi National Open University) which is an academic organisation (.ac) and is situated in country India (.in).

Check Your Progress 3

1. What are the services on Internet?

…………………………………………………………………………………………

…………………………………………………………………………………………

2. What is firewall? Where can it be used?

…………………………………………………………………………………………

…………………………………………………………………………………………

3. What it TCP/IP? Why is it used?

…………………………………………………………………………………………

…………………………………………………………………………………………

4. What is a URL?

…………………………………………………………………………………………

…………………………………………………………………………………………

5. Define the terms DSN, IPv4 address, Subnet mask

…………………………………………………………………………………………

…………………………………………………………………………………………

1.10 SUMMARY

This unit is an effort to answer some of the very basic questions about the data communications, networking and the Internet. The Unit first defines the term networks, while discussing its advantages and disadvantages. It also defines the term Internet. Some of the basic terminology of data communications like modes of transmission, speed of transmission, packet etc has also been defined. To communicate data, you require some channel. This unit provides details on the Guided and unguided data transmission channels. Network topologies define the basic structure of the network. Three basic network topologies – bus, ring and star have been defined in this Unit. The networks can also be classified on the basis of their characteristics. LANs are the networks that cover a range of few Kilometers whereas MANs cover a range of about 50 Kilometers. The WANs have the largest range. On the other hand, the speed of transmission of data decreases from LAN to WAN as you can employ better, faster but costlier technology at short distances. The unit also covers the reference models that may define the networking software. In addition, the unit discusses about some of the basic devices used in Computer Network. These devices are - Network Interface Card, Modem, Repeaters, Bridge, Hub, Switches, Router and Gateway. The Unit also explains the IP addresses, DNS and email based addresses. One of the most important addresses for Internet user is Uniform Resource Locator that uniquely identifies a document or resource on the Internet. Networking and Internet is a very dynamic area and newer technologies emerge very fast in this area. Therefore, you must update yourself on various newer concepts on these topics from the further readings.

1.11 ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress 1

1. Computer networks are manly used for the purpose of resource sharing which helps in reducing organizational costs. Networks are highly reliable, scalable and very powerful communication system.
2. MODEM is an encoder as well as decoder it converter digital signal to analog at the source and analog signal back to digital at the destination.
3. The performance of the twisted pair can be improved by adding a metallic shield around the wires. Shielded wires are much more resistant to thermal noise and crosstalk effects.
4. An optical fiber consists of two concentric cylinders: an inner core surrounded by a cladding. Both the core and the cladding are made of transparent plastic or glass material. Optical fiber use reflections to guide light through a channel. The density of core and cladding must differ sufficiently to reflect the beam of light instead of refracting. The core is used for guiding a light beam, whereas the cladding (which has a different refractive index) acts as a reflector to prevent the light from escaping from the core. Optical Fiber has high bandwidth and does not suffer from noise. However, it is costly and requires experts to do the connections.

Check Your Progress 2

1. The basic characteristic of topology is its organization. This leads to properties that may be used to differentiate them. Some of these characteristics are: Network Scalability, Cost, Length of Cable etc.
2. LAN – about 2 Kms it is high speed network; MAN up to 50 Kms - may use devices like Modem; WAN – covers large distances like states countries.

3. LAN – Network in a University, Small office, Internet Cafes

   MAN – Cable TV network

   WAN – Internet, VPN etc.

4. A bridge connects several LANs. A bridge can also divide a network to isolate traffic or problems. Bridge Interconnects LAN segments at the network interface layer level and forwards frames between them.

   A router translates information from one network to anther; it is more intelligent than a bridge. Routers select the best path to route a message, based on the destination address and origin. In contrast to bridges few of the large routers may include programs for their operations.

5. A hub is the simplest of connection devices. Any data packet coming from one port is sent to all other ports. It is then up to the receiving computer to decide if the packet is for it. A hub is typically the least expensive, least intelligent, and least amount of date going across the network is network is never very high.

6. Gateway Interconnects networks at higher layers than bridges or routers. A gateway usually supports address mapping from one network to another, and may also provide transformation of the data between the environments to support end-to-end application connectivity. The main functionality of a gateway is to convert protocols among communications networks. A gateway on the other hand can accept a packet formatted for one protocol and convert it to packet formatted for another protocol before forwarding it. Gateways work on all seven OSI layers.

Check Your Progress 3

1) Today you can avail the facilities of e-mail; messenger services, Chatting etc., to share your ideas, knowledge, and feeling. You can join different groups, discussion forums or create your own blogs. You can use websites to broadcast huge amount of information on Internet.

2) Firewall is software that works on some set of rules and instructions given by you. A firewall helps to keep your computer more secure and protect from many security problems like; hacking, Trojan Horse, Virus, etc. It restricts information that comes to your computer from other computers, giving you more control over the data on your computer and providing a line of defense against people or programs (including viruses and worms) that try to connect to your computer without invitation.

3) A stack of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol) implements different rules to handle the data communication from source machine to destination machine. For sending a message from source machine to destination machine, TCP divides the message data into little data packets. It also adds special information e.g., the packet position, error correction code etc., to make sure that packets at the destination can be reassembled correctly and without any damage to data. The role of IP here is to put destination-addressing information on such packets. On Internet it is not necessary that all the packets will follow the same path from source to destination A special machine called routers tries to, load balance various paths that exist on networks. Other special machine called gateways allows different electronic networks to talk to Internet that uses TCP/IP.

4) A URL is a unique identifier for a resource on Internet.

5) DNS is responsible for Web addresses to IP address; IPv4 address is a 32 bit address of a host on Internet. Subnet mast separates Network ID and Machine ID.

1.12 FURTHER READINGS

- CIT-001-*Fundamentals of Computer System*, Block 3 : *Networking and Communication*, Block Preparation team : Sh. Shashi Bhushan (Content editor) and Shri Saurabh Shukla
- CIT-001 : *Web based Technologies and Multimedia Applications*, Block-1 : Internet Concepts, Block Preparation Team – Prof. M.N. Dooja (Content Editor), Dr. Pramod Kumar (Language Editor), Dr. R. Khandwal, Mr. Hemant Rana, Dr. Naveen Kumar, Mr. Akshay Kumar.
- A.S. Tanenbaum, *"Computer Networks"*, Pearson Education Asia, 4th Ed.
- Behrouz A. Forouzan, *"Data Communications and Networking"*, Tata Mcgraw-Hill.
- William Stallings, *"Data and Computer Communications"*, Sixth Edition, Prentice Hall.
- Behrouz A. Forouzan, *"TCP/IP Protocol Suit"*, Tata Mcgraw-Hill
- D.E. Comer, 2001 *"Internetworking with TCP/IP"*, Pearson Education Asia.
- Comer E. Doughlas, 2000 *"Computer Networks and Internets"*, 2nd Ed., Pearson.
- Laura Chappel(Ed), 99*"Introduction to Cisco Router Configuration"*, Techmedia.
- Alexis Leon and Mathews Leon(1999), *Fundamentals of Information Technology*, Leon TechWorld publication.
- PK Sinha & Priti Sinha, *"Foundations of Computing"*, BPB Publication.
- Dr. Larry Leng(2004), *Computer Fundamental*, Wiley Dreamtech Publication.
- Suresh K. Basandra(2003), *Computer Today*, Galgotia publication.
- Thomas A. Powell, *Web Design: the complete reference*, Tata Mc. Graw-Hill, 2004

References websites

- http://www.brainbell.com/tutorials/Networking/
- http://www.networktutorials.info/
- http:// www.nethistory.info/
- http://en.wikipedia.org/wiki/Modem
- http://en.kioskea.net/contens/transmission/transmode.php3
- http://brainbell.com
- http://eiu.edu
- http://neiu.edu
- http://public.pacbell.net/faq/general_faq.html
- www.unf.edu/library/guides/search.html
- www.lib.berkeley.edu/TeachingLib/guides/Internet/SearchEngines.html
- www.sc.edu/beaufort/library/pages/bones/lesson7.shtml
- http://mail.google.com/support/?hl=en
- http://help.yahoo.com/l/us/yahoo/messenger/messenger8/index.html
- http://en.wikipedia.org/wiki/wiki